

# Top Tips for keeping your personal data safe online



An Coimisiún um  
Chosaint Sonrai  
Data Protection  
Commission

When you go online, you leave a digital footprint behind you. This footprint is like a record of how you behave on the internet and is based on things like your activities online (e.g. the websites you visit, what you click on) but also the personal data you share. Taking just a few simple steps whenever you go online will really help you keep your data much safer.

## 1. Check your social media profile settings



The Data Protection Commission (DPC) recommends that social media accounts for under 18s should automatically be set to "private", which means that only your friends can see what you like, post and share. If your profile on a social media platform is already "public" or you change it to "public" then everyone and anyone can see what you're sharing and talking about online or send you messages. Always think very carefully about switching off any privacy controls that are there to keep you safe.

## 2. Think before you post



Whether your profile is set to public or private, remember that once you post something online it can be really hard to delete it completely from the internet. So before you post, ask yourself if this is something you really want everyone to see for years to come.

## 3. Treat other people's data the way you would treat your own



Listen to your friends or family if they ask you to take down pictures or videos of them. You might want them to do the same for you one day!



#### 4. Be careful tagging yourself or “checking in”

Sharing your location online can be risky so turn off your location settings if you don't need them. Think twice about checking into places or tagging yourself as somewhere.



#### 5. Don't let yourself be “nudged”

Sometimes, apps and platforms try to “nudge” you into handing over more information than they actually need. Maybe the button they want you to click on is big, bright and in the middle of the screen while the other option is tiny and easy to miss. Watch out for these tactics and choose the option that you're most comfortable with, not just the one that's easiest to click on.



#### 6. Read the terms and conditions (as best you can)

Companies should give you information about what it is they do with your personal data. That information should be written in plain English that you can easily understand and should be easy for you to find. Ask a parent or trusted adult if you are unsure about anything.



#### 7. Don't just click “Accept all”

The next time you see a privacy notice or a cookie banner, think about whether you want to change the settings rather than just clicking on “accept all” cookies. Look for the button that allows you to reject any cookies that are not needed or essential. Otherwise you may be agreeing to share more information than you would like or realise.



## 8. Know the value of your data

"Free" services aren't always free. A lot of the personal data we share online is used by companies to make money from things like advertisements. Always ask yourself "Am I getting a fair deal here?"



## 9. Remember, you are in control

You have rights when it comes to your personal data. Online platforms and companies have to listen to you if you want a copy of your data or want to delete your social media.



## 10. Keep your parents in the loop

Even if you're in control of your personal data, it's always a good idea to keep your parents or a trusted adult in the loop and to ask for their help if you need it. Never lie about your age or pretend to be your parent when signing up for social media!



## 11. Delete it when you're done

Don't leave accounts open that you no longer use. They could get hacked and be used to break in to your other accounts, especially if you have weak passwords.



## 12. Don't use the same password for everything!

That just makes it too easy for your data to be stolen. Never use the same password twice and keep them as unusual and original as possible. Don't base your passwords on obvious things that someone else could guess, like your pet's name or your favourite TV show. Use a password manager if you can.



## 13. If it looks dodgy, don't click on it.

Did you get a fishy message from a stranger or even a friend? It could be a scam of some kind. Don't open it, don't click on any links and delete it straight away. Better safe than sorry.



## 14. Never use unsecured Wi-Fi.

It may seem easy because you can just click and join but unsecured networks are very risky. A hacker using the same network could use it to steal your data or even take control of your device!



## 15. Keep your devices up to date!

It's always tempting to click "remind me later" when you're asked to install an update. But these updates often contain important protections against the latest viruses and scams. Always install updates as soon as possible.

### Get in touch

If you have any questions about protecting your personal data, you can contact the Data Protection Commission and we'll be happy to answer your questions. You can call us on 01 7650100 or 1800437 737. You can also contact us by post or email. For information on how to get in touch, check out our website: <https://www.dataprotection.ie/en/contact/how-contact-us>

